CRA SAMPLE

D04 Control and safety concept

Blank template · Nordwald Wärmetechnik GmbH, networked wood chip boiler NWT HACKTHERM 60 connect

Publisher	OT-Cyber.de, Max Gilg, Rosenheim
Sample company	Nordwald Wärmetechnik GmbH, networked wood chip boiler NWT HACKTHERM 60 connect (fictitious)
Note	Free sample, not legal advice

Fill in the fields, approve with date and signature, file according to document control.

1 Purpose and scope

Safety controller, basic design decisions, safety functions with PLr according to EN ISO 13849-1, achieved PL and validation. Shows that safety is maintained without software and without the network.

How to fill in this form

Fill in the fields with the details of your company. Below each table and next to each field there is an example from the sample company for orientation. Refer to evidence by number (e.g. ticket or form). Finally approve with date and signature and file according to document control.

2 Document control

Field	Entry
Document no.	
Version, status	
Scope	
Author	
Checked by	
Approval	
Next review	
Confidentiality	
Filing	

3 Control and safety concept: overview

Field	Entry	Example from the sample
Safety controller		Siemens SIMATIC S7-1200 G2, CPU 1214FC G2 with …
F-program		Version 3.0.0, collective signature on file, …

4 Principles

	Punkt	Wer / bis wann
☐	G1: STL, thermal discharge safety device, safety valve and extinguishing system work without software and without the network	
☐	G2: No remote access to F-data, the gateway has no write access	
☐	G3: Values passed from the standard program to the F-program are checked against fixed limits	
☐	G4: No hazardous restart without a closed interlock and local acknowledgement (MR, Annex III, section 1.2.6)	

5 Safety functions: how reliable each one must be

How to read the table

For each safety function we answer three questions according to EN ISO 13849-1. S: How severe would the injury be if the function failed? F: How often is someone exposed to the hazard? P: Can the person still avoid it? The three answers give the required Performance Level PLr, from a (low) to e (very high). The control system must reach at least this value; the column 'PL achieved' shows this. The category states how the control system is designed to achieve it.

SF	Safety function	S	F	P	PLr	Cat.	PL achieved	Validated (F09)

Example row from the sample: SF: SF1 · Safety function: Burn-back protection: rotary valve … · S: S2 · F: F1 · P: P2 · PLr: d · Cat.: 3 · PL achieved: d · Validated (F09): 02.03.2027

Legend: SF = safety function; S = severity of injury: S1 slight, S2 serious or fatal; F = frequency or duration of exposure: F1 rare, F2 frequent; P = possibility of avoiding the hazard: P1 possible, P2 scarcely possible; PLr = required performance level according to EN ISO 13849-1 (a to e); Cat. = category, the structure of the control system from B (simple) to 4 (dual channel with self test).

6 How we use the table

…

…

…

Example from the sample: Example SF1 burn-back protection: a burn-back into the storage room can cause serious injury (S2), someone is rarely …

7 Control system architecture

Field	Entry	Example from the sample
Category 3		two channels via F-DI with cross-circuit …
Category 2		the F-CPU tests the function at start-up and …
Parameters for PL d		probability of dangerous failure PFHd below …

Describe your status here, specifically and with a date. Example from the sample: Standard program 3.0.3 (NWT-CHG-2027-005) only optimised the burner control.

8 Terms and abbreviations

CHG: change request (number range)

CPU: processing unit of the controller

F-AI: fail-safe analogue input

F-DI: fail-safe digital input

F-DQ: fail-safe digital output

MR: Machinery Regulation (EU) 2023/1230, applies from 20 January 2027

NWT: abbreviation of the sample company in document and ticket numbers

PFHd: average probability of a dangerous failure per hour

PL: performance level according to EN ISO 13849-1, from a (low) to e (high)

PLr: required performance level

SF: safety function

STL: safety temperature limiter

9 Revision history and approval

Version	Date	Change	Approval

Version	Date	Change	Approval

Approved (name, function, date, signature): _____ · Free sample from OT-Cyber.de, not legal advice. Company, persons, serial numbers and data are entirely fictitious.